

# Comment renforcer votre défense contre les maliciels et protéger votre PC

Pour protéger votre ordinateur contre les programmes malveillants :

- [Renforcez les défenses de votre ordinateur](#)
- [Ne vous laissez pas tenter par un téléchargement de programme malveillant](#)

## Renforcez vos défenses contre les programmes malveillants

### Installez les programmes anti-virus et anti-espion d'une source de confiance

- Ne téléchargez jamais rien suite à un avertissement d'un programme que vous n'avez pas installé ou que vous ne reconnaissez pas et qui prétend protéger votre PC ou offre de supprimer des virus. Il est fort probable que ce programme ait l'effet opposé.
- Obtenez des programmes anti-maliciels réputés auprès d'un éditeur auquel vous faites confiance.
  - [Microsoft Security Essentials](#) offre la protection de votre PC en temps réel gratuite contre les logiciels malveillants.
  - OU [choisissez dans une liste de partenaires Microsoft](#) qui fournissent des logiciels anti-maliciels.

### Mettez à jour vos logiciels régulièrement

Les cybercriminels font preuve d'un esprit inventif sans relâche pour exploiter les vulnérabilités des logiciels, et de nombreuses sociétés informatiques travaillent inlassablement pour lutter contre ces menaces. C'est pourquoi vous devriez :

- Installer régulièrement des mises à jour pour tous vos logiciels : programmes anti-virus et anti-espion, navigateurs (par exemple Windows Internet Explorer), systèmes d'exploitation (comme Windows) et traitement de texte et autres programmes.
- Abonnez-vous à des mises à jour automatiques des logiciels lorsqu'elles sont offertes, par exemple, vous pouvez [mettre à jour automatiquement tous les logiciels Microsoft](#) .
- Désinstallez les logiciels que vous n'utilisez pas. Vous pouvez les supprimer à partir du Panneau de configuration de Windows.

### Utilisez des mots de passe forts et gardez-les secrets

- Les mots de passe forts font au moins 14 caractères et comprennent un mélange de lettres, de chiffres et de symboles. Apprenez comment les créer.
- Ne communiquez vos mots de passe à personne.
- N'utilisez pas le même mot de passe sur tous les sites. S'il est volé, toutes les informations qu'il protège courent des risques.


- Créez différents mots de passe forts pour le routeur et la clé sans fil de votre connexion sans fil familiale. Renseignez-vous auprès du fabricant de votre routeur.

### **Ne désactivez jamais votre pare-feu.**

Un pare-feu place une barrière de protection entre votre ordinateur et Internet. Le fait de l'inactiver même une minute augmente le risque que votre PC soit infecté par un programme malveillant.

### **Utilisez les lecteurs flash avec précaution**

Minimisez les chances d'infection de votre ordinateur par des programmes malveillants :

- Ne branchez pas de lecteur flash inconnu (clé USB) sur votre PC.
- Maintenez la touche MAJ enfoncée lorsque vous insérez la clé dans votre ordinateur. Si vous oubliez de faire ça, cliquez sur  dans le coin supérieur droit pour fermer toute fenêtre pop-up relative au lecteur flash.
- N'ouvrez pas de fichier de votre lecteur auquel vous ne vous attendez pas.

## Ne vous faites pas duper à télécharger un programme malveillant

Suivez plutôt ce conseil :

- Faites très attention lorsque vous ouvrez des pièces jointes ou que vous cliquez sur des liens dans des messages électroniques ou instantanés, ou dans des publications de réseaux sociaux (comme Facebook), même si vous connaissez l'expéditeur. Appelez pour savoir si c'est bien un ami qui l'a envoyé ; si ce n'est pas le cas, supprimez-le ou fermez la fenêtre de messagerie instantanée.
- Évitez de cliquer sur **D'accord, OK**, ou **J'accepte** dans les bannières publicitaires, dans les fenêtres ou avertissements pop-up inattendus, sur des sites Web qui n'ont pas l'air légitimes, ou dans les offres de suppression de logiciels espions ou de virus.
  - Appuyez sur **CTRL + F4** sur votre clavier.
  - Si la fenêtre ne se ferme pas, appuyez sur **Alt + F4** sur votre clavier pour fermer le navigateur. Si une invite vous le demande, fermez tous les onglets et n'enregistrez aucun onglet pour le prochain démarrage du navigateur.
- Ne téléchargez de logiciel que de sites Web dignes de confiance. Méfiez-vous d'offres de musique, jeux, vidéos, etc. « gratuits ». Il est de grande notoriété qu'ils renferment des programmes malveillants dans le téléchargement.